NAVAL WAR COLLEGE
Newport, R.I.

ADDRESSING THE LEGAL CHALLENEGES OF NETWORK CENTRIC WARFARE
Case In Point:
The Legal Implications of Obtaining an "Information and Knowledge Advantage" Prior to Hostilities

Sean P. Henseler
Lieutenant Commander, United States Navy, JAGC

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: Sean P. Henseler

5 February 2001

Abstract

ADDRESSING THE LEGAL CHALLENEGES OF NETWORK CENTRIC WARFARE
CASE IN POINT:
THE LEGAL IMPLICATIONS OF OBTAINING AN "INFORMATION AND KNOWLEDGE ADVANTAGE" PRIOR TO HOSTILTIES

If it is true that the Navy is moving away from platform-centric toward network-centric warfare (NCW), then its leaders must ensure that any such transition is accomplished in the most efficient and effective manner possible. Since the Navy's current vision of net-centric operations raises many complex and often unsettled legal issues, the Navy must establish a formal framework for analyzing the legal challenges posed by NCW then integrate this framework into any NCW transition process.

Future net-centric operational commanders have a vested interest in ensuring that the legal implications of NCW on factor space, time, and forces have been thoroughly considered. Current and future international and domestic law might limit the ability of net-centric commanders to optimize the key concepts of the Navy's vision of net-centric operations. If the technological and doctrinal aspects of NCW continue to rapidly evolve without regard for the legal challenges, the Navy might find itself in a position where it has invested a tremendous amount of time and money developing a system of sensors and platforms that cannot be employed as envisioned due to legal constraints.

The time is now to begin systematically considering the legal challenges posed by NCW. Lessons from the past have shown that technology, doctrine, and organization should not evolve autonomously. Rather, the more prudent course is to provide for the co-evolution of this triumvirate. Part of this co-evolution entails a rigorous legal analysis of the underlying concepts of NCW. As such, a formal framework to integrate this legal analysis into the ongoing evolution of NCW is mandatory and the appropriate resources should be applied.

NWCR-A

3

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification): ADDRESSING THE LEGAL CHALLENGES OF NETWORK CENTRIC WARFARE Case in Point: The Legal Implications of Obtaining an "Information and Knowledge Advantage" Prior to Hostilities (U)

9. Personal Authors: SEAN P. HENSELER, USN, JAGC, LCDR

10. Type of Report: FINAL

11. Date of Report: 5 Feb 2001

12. Page Count: 27

12A Paper Advisor (if any): CDR Audrey Bogle, USCG

13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper: NETWORK, CENTRIC, WARFARE, LEGAL, CONSIDERATIONS, INFORMATION, SUPERIORITY, KNOWLADGE, SENSOR, GRID

15. Abstract:

If it is true that the Navy is moving away from platform-centric toward network-centric warfare (NCW), then its leaders must ensure that any such transition is accomplished in the most efficient and effective manner possible. Since the Navy's current vision of net-centric operations raises many complex and often unsettled legal issues, the Navy must establish a formal framework for analyzing the legal challenges posed by NCW then integrate this framework into any NCW transition process.

Future net-centric operational commanders have a vested interest in ensuring that the legal implications of NCW on factor space, time, and forces have been thoroughly considered. Current and future international and domestic law might limit the ability of net-centric commanders to optimize the key concepts of the Navy's vision of net-centric operations. If the technological and doctrinal aspects of NCW continue to rapidly evolve without regard for the legal challenges, the Navy might find itself in a position where it has invested a tremendous amount of time and money developing a system of sensors and platforms that cannot be employed as envisioned due to legal constraints.

The time is now to begin systematically considering the legal challenges posed by NCW. Lessons from the past have shown that technology, doctrine, and organization should not evolve autonomously. Rather, the more prudent course is to provide for the co-evolution of this triumvirate. Part of this co-evolution entails a rigorous legal analysis of the underlying concepts of NCW. As such, a formal framework to integrate this legal analysis into the ongoing evolution of NCW is mandatory and the appropriate resources should be applied.

16. Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		

17. Abstract Security Classification: UNCLASSIFIED

18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19. Telephone: 841-6461

20. Office Symbol: C

Security Classification of This Page Unclassified

Introduction

In a 1997 address to the U.S. Naval Institute, then-Chief of Naval Operations (CNO) ADM Jay L. Johnson, USN, asserted that the military was in the midst of a "fundamental shift from what we call platform-centric warfare to something we call network-centric warfare."[1] More recently, VADM Arthur K. Cebrowski, President of the Naval War College, hailed NCW as "the emerging military response to the information age" whose "time is at hand."[2] If these two distinguished naval leaders are correct, then the Navy may soon have to significantly change the way it trains, organizes, and allocates its resources.[3] Indeed, the process of experimenting with NCW concepts in wargames and fleet exercises has already begun.

If it is true that the Navy may radically alter its approach to warfare, then its leaders must ensure that any transition to NCW is accomplished in the most efficient and effective manner possible. Since the Navy's current vision of NCW raises a multitude of thorny and often unsettled legal issues, the Navy must establish a formal framework for analyzing the legal challenges posed by NCW then integrate this framework into any NCW transition process.[4]

Today we already have a solid foundation for pushing nascent NCW technology and doctrine to the fleet via wargames, Fleet Battle and Sea Dragon Experiments, Joint Warfare Interoperability Demonstrations, the Marine Corps Fighting Lab, the Strategic Studies Group, and a revamped Naval War College.[5] However, while there has been some limited participation by legal experts in these exercises and entities, particularly with regards to Rules of Engagement (ROE), in order to ensure the most efficient development of Navy net-centric doctrine a more formal, expansive, coordinated and focused effort is needed. The

lack of coordinated legal analysis at the outset of the Navy's possible transition to NCW is especially disturbing given that the U.S. has a "particularly significant stake in understanding how international and domestic law will apply to information age forms of conflict."[6]

In an effort to highlight the importance of establishing a formal framework to legally review the Navy's evolving vision of net-centric operations, this article will focus on one key component of NCW: information superiority.[7] Specifically, this article will analyze the legal issues posed by the Navy's current "Capstone Concept" for naval operations in the information age which envisions gaining an "Information and Knowledge Advantage" over possible adversaries by installing an Expeditionary Sensor Grid (ESG) inside their territory, territorial seas, and airspace preferably *before* they have committed a hostile act.[8] After analyzing the legal implications of installing this grid *prior* to the outbreak of hostilities, this article will briefly discuss other legal challenges posed by NCW and offer recommendations as to how legal experts might more actively participate in the development of NCW as it relates to the Navy. Finally, this article concludes that, should the Navy continue to transform toward NCW, it must provide for the systematic legal analysis of the underlying concepts of net-centric operations to ensure the most efficient evolution of NCW technology and operational doctrine.

Gaining an Information/Knowledge Advantage by Installing an ESG Prior to Hostilities

According to the Naval War College's "Network Centric Operations: A Capstone Concept for Naval Operations in the Information Age," Navy forces of the future will execute network-centric operations using four major supporting concepts: Information and Knowledge Advantage, Assured Access, Effects-Based Operations, and Forward Sea-Based

Forces.[9] Of these four elements, information and knowledge advantage is *the* central element that enables and connects the other concepts.[10]

Evolving Navy net-centric doctrine holds that in the network-centric era one of the operational commander's first actions would be to employ "a range of sensors to expand the existing knowledge base" so as to "build an information advantage over the adversary."[11] Perhaps the most critical means of obtaining this "information advantage" would be via what has been labeled the Expeditionary Sensor Grid (ESG).[12]

As envisioned, this multi-tiered ESG would combine both theater and national sensors with numerous organic tactical sensors that could dwell in and over adversary territory.[13] The upper level, resident in satellites or very high-flying unmanned aerial vehicles (UAVs) would provide broad surveillance, communications support, and initial cueing for other sensors.[14] Additionally, large numbers of mid and low-level sensors that could "get close in" would provide weapons-quality tracking, identification, and detailed effects assessment and could be armed to deal with time-critical targets provide in-flight updates to networked weapons.[15] Specialized ground, surface and undersea sensors in every operating domain would compliment airborne sensor tiers.[16]

In addition to installing an ESG, in order to obtain information superiority network-centric operational commanders would also simultaneously "use offensive information operations to degrade the opponent's information systems and networks."[17] The result for a potential adversary would be a "vicious circle in which he has growing demands to expand his knowledge at the same time that he is losing sensor and weapons capabilities."[18]

From an operational perspective, Navy net-centric doctrine calling for the installation of an ESG, coupled with simultaneous information operations in order to gain information

superiority might appear to be a desirable course of action. However, arguably the *legality* of this course of action becomes questionable if the operational commander were to employ his sensors inside a sovereign nation's territory, territorial seas, and/or airspace (not to mention conduct simultaneous information operations) *before* his potential adversary had clearly demonstrated hostile intent or committed a hostile act. This is the crux of the legal challenge posed by the information superiority component of the Navy's net-centric concept of operations which holds that sensor access will be both stealthy and enduring both *prior to hostilities and in operations other than war.*[19]

A Scenario Where an ESG Might be Installed

Current Navy net-centric doctrine doesn't propose that operational commanders will install ESG's inside sovereign nations during the 'normal' peacetime environment. Rather, ESG's would likely only be established within a geographic area where a developing crisis could significantly threaten U.S. interests. Taken as a whole, the concept of NCW places a heavy emphasis on deterring an armed conflict before it truly begins. Arguably, the ultimate goal of NCW is "to stop something before it starts."[20] As such, one implication NCW has for policymakers and operational commanders is the "need to consider *proactive* and *early* combat operations as a means to deter conflict or contain crisis situations before they expand."[21]

For the purposes of this article let us consider the following scenario. Suppose there existed *some* indications that Country *X* might initiate an armed attack against a nearby nation in which U.S. forces are based overseas (sometimes referred to as ambiguous warning). In such a situation a future net-centric Joint Task Force (JTF) commander could be faced with a decision whether or not to install an ESG in order to obtain more concrete

information that Country *X* actually possessed the capability and intent to launch an armed attack (sometimes referred to as unambiguous warning). Moreover, the JTF commander might wish to install an ESG to facilitate possible follow on responses. Let us further assume that there are no applicable U.N. resolutions or regional defense treaties in place that could provide a legal basis for installing the ESG.

Arguably, in the above scenario, under current doctrine it is highly unlikely that a JTF commander would install an ESG without approval from higher authority. Thus, the burden in the near term will likely fall on the National Command Authority (NCA) to decide whether or not to install an ESG prior to hostilities. However, in the future, given the anticipated increased speed of warfare, NCW's reliance on self-synchronization, and the tremendous destruction that could be caused by an enemy first salvo, operational commanders may well be 'on the hook' to make such a critical decision.

Legal Implications of Installing an ESG Prior to Hostilities

Historical evidence suggests that before approving the installation of an ESG the NCA would likely scrutinize all of the legal implications of such a provocative act.[22] As will be shown below, legal arguments can be made both in opposition to and in support of the legality of installing an ESG inside a sovereign nation's territory, territorial seas, and/or airspace prior to the outbreak of hostilities. Despite the fact that below appear but two of many possible legal arguments, the reader should be cautioned that, in any case of difficulty,

> "...it is not possible to say categorically in advance whether a proposed course of action is 'lawful' or not. Partly this is because legal consequences...are very sensitive to nuances of the fact setting and the concrete details of the challenged activity...which...do not emerge until the action is taken. The relevant facts are, in a sense, defined by the action. Thus, no lawyer...can give a definitive opinion as to the legality of conduct in advance...Legal advice must come to the client in the form of an assessment of risks and probabilities..."[23]

Notwithstanding the preceding disclaimer, the first step in conducting any analysis regarding the legality of installing an ESG inside a sovereign nation prior to hostilities is to determine the applicable law. The next step is to apply the law to the particular facts of the case. In the context of the scenario outlined above one would consider the applicable international law, which includes international treaties, conventions and agreements as well as customary international law.[24] Additionally, one might also look to opinions from international courts, tribunals or expert treatises if relevant. Finally, one would also consider whether or not any domestic or foreign national laws were pertinent to the issue.

In the scenario above the main bodies of law that one would likely consider include the law of the sea, laws regarding espionage and intelligence collection, and the law pertaining to a nation's right to take actions in 'self-defense.' As noted previously, by stressing one body of law over another and/or by focusing on certain critical facts in the scenario, an attorney could craft a legal argument on either side of the ESG installation issue. Indeed, lawyers rarely look for or expect to find clear answers.[25] More often than not, lawyers search their "data base- treatises, articles, statutes, cases, and other materials- in order to construct legally acceptable arguments in pursuit of one or more objectives."[26] However, in the final analysis, in today's post-Cold War global environment the NCA would probably attempt to justify its chosen course of action by stressing the legal argument that would most likely persuade the majority of foreign and domestic observers that its actions were legal.[27]

Argument 1: Installing an ESG Prior to Hostilities Would Be Unlawful

The starting point for this argument would be an assertion that the installation of an ESG inside the territory, territorial sea or airspace of Country *X* when there were *merely* some indications of a future armed attack would constitute an attempt to *collect intelligence utilizing technical platforms during peacetime.* In general, intelligence collection is a

continuous process of gathering information and is an international norm.[28] "It is not limited to information not publicly available, nor necessarily derived from information that is concealed or not intended to be available to the collector."[29] Indeed, much information is collected from open sources. As such, intelligence collection *per se* does not violate international law.[30]

Of note, most nations endeavor to deny intelligence gathering within their territory through domestic laws and no serious proposal has been made within the international community to prohibit the *concept* of intelligence collection as a violation of international law given the tacit acknowledgement that it is important to all and practiced by each.[31] However, some aspects of international law affect the *means* to be utilized in collection.[32] A leading example is the sovereign right of each nation to control access to its territory, coastal waters, and the airspace above each; and to limit the activities within each.[33]

As such, the applicable law in the scenario above would include areas of *peacetime* international law dealing with the sovereign rights of nations over their territories, coastal waters, and the airspace above each, the law of the sea, and the Charter of the United Nations. For purposes of clarity this article will address the legality of each tier of the ESG in turn then briefly discuss possible remedies that might be available to Country *X*.

Surface and subsurface sensors: Current Navy net-centric doctrine envisions utilizing various manned and unmanned sensors to gather intelligence on and under a target area's seas. With respect to sensors on and under the territorial sea of Country *X*, anyone challenging the lawfulness of the ESG would argue that the controlling law would be found in the United Nations Convention on the Law of the Sea. Of note, despite the fact that the U.S. has not yet ratified the Law of the Sea Convention, it has formally stated that the

convention, in its pertinent parts, is a codification of customary law and thus binding on the U.S.[34] Of particular relevance to the scenario at hand, the Law of the Sea Convention not only defines what comprises a nation's territorial sea (and airspace) but also proscribes the rules that apply to all ships and submarines that may desire to enter another nation's territorial seas.

In general, a coastal state's sovereignty extends to the sea and airspace out to 12 nautical miles from its land territory.[35] Strictly interpreted, the Law of the Sea Convention would only vest in the U.S. the right of "innocent passage" through the territorial sea of Country *X* in our scenario's 'peacetime' environment.[36] The right of innocent passage explicitly precludes: 1) any act claimed at collecting information to the prejudice of the defense or security of the coastal state, 2) the launching, landing, or taking on board of any aircraft or military device, 3) any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal state, and 4) any activity not having a direct bearing on passage.[37] Moreover, in the territorial sea submarines and other underwater vehicles are required to navigate on the surface and to show their flag.[38] Finally, the Law of the Sea Convention specifically authorizes states "to lay submarine cables" only on the "bed of the high seas beyond the continental shelf."[39]

Given the above prohibitions, and the fact that the Law of the Sea Convention was prompted by a desire to settle "all issues…relating to the law of the sea," one could argue that clearly the installation of an ESG inside the territorial seas of Country *X* would violate the spirit, if not the letter, of the Law of the Sea Convention.[40]

Airborne sensors: Pursuant to the Law of the Sea Convention and Article I of the Convention on International Civil Aviation (1944), every nation has complete and exclusive

sovereignty over the airspace above its territory, its internal waters, its territorial sea, and, in the case of an archipelagic nation, its archipelagic waters.[41] This sovereign right includes the right to regulate and/or deny access.[42] Article 3 of the Convention on International Civil Aviation provides that "(a)ircraft used in military…service shall be deemed state aircraft. No state aircraft…shall fly over the territory of another state or land thereon without authorization."[43] Unlike ships, aircraft have no right of innocent passage and by implication intelligence collection is prohibited.[44]

Penetration of a state's airspace without permission for purposes of collecting intelligence, while often vaguely characterized as 'a violation of international law,' more correctly may be regarded as a violation of the sovereignty of that state *as recognized by* international law.[45] As such, if the U.S. were to fly aircraft or UAV's inside the national airspace of Country *X* without its permission it would be clearly in violation of Country X's sovereignty.

Ground sensors: Ground sensors could only be installed lawfully within Country *X* with its permission. Any other placement of ground sensors inside the territory of Country *X* would be in violation of its sovereignty.

A final argument that the installation of an ESG inside the territory of Country *X* prior to hostilities would be unlawful results from the application of the notion of reciprocity. Simply put, a pertinent question that must be asked is, "How would the U.S. view the placement of an ESG inside *its* territory prior to it demonstrating hostile intent or committing a hostile act?" More than likely the U.S. would view any such action as a violation of its sovereignty and would respond in necessary and proportional fashion.

Remedies available to Country X: In determining whether or not installing an ESG was lawful, a lawyer would also consider the remedies available to Country *X* given U.S. actions. While a complete discussion of the possible 'lawful' remedies available to Country *X* if it found an ESG 'unlawfully' installed inside its territory prior to hostilities is beyond the scope of this paper let us briefly consider the issue.

First, Country *X* would argue that it had not threatened or used force against any entity in violation of Article 2(4) of the U.N. Charter which states that all "(m)embers shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[46] Thus, the U.S. could not justify its actions pursuant to Article 51 of the U.N. Charter which states that the "inherent right" of "self-defense" only arises after an "armed attack occurs against a Member of the United Nations."[47] Second, Country *X* would argue that the U.S had violated its sovereignty as recognized in the Law of the Sea Convention, the Chicago Convention, and customary international law and was thus entitled to remove the grid, by force if necessary. Lastly, *Country X* could also argue that the installation of the ESG represented a "threat or use of force" *on the part of the U.S.* as defined in Article 2(4) of the U.N. Charter. Characterized in this manner, Country *X* might also be successful in persuading a worldwide audience that physical elimination of the ESG would be justified as an act of "self-defense" pursuant to Article 51 of the U.N. Charter.

Past historical examples such as the Soviet shoot-down of a U.S. U-2 in 1960, its dropping of depth charges on submarines 'caught' inside Soviet territorial seas, and Sweden's dropping of depth charges against suspected Soviet submarines in Swedish

territorial waters highlight the stark reality that nations will respond militarily if they believe their sovereignty has been violated.[48]

Certainly, the U.S. has in the past factored into its decision-making process the possibility that its intelligence collection assets might be militarily engaged if 'caught' inside other nation's territorial waters or airspace.[49] Aware that a U.S. U-2 had been shot down over the Soviet Union in 1960, and that a Chinese Nationalist U-2 had been shot down over Red China on September 9, 1962, the U.S. briefly suspended hi-altitude reconnaissance flights over Cuba during the 1962 Cuban Missile Crisis. Certainly, during that 'crisis' situation, policymakers strongly desired 'unambiguous' evidence that the Soviet Union had placed offensive nuclear missiles inside Cuba. However, there was a tacit recognition by the U.S. that entry into Cuban airspace might violate Cuba's sovereignty and that Cuba might be justified if it shot down a U-2.[50] Then-Secretary of State Dean Rusk thus had his legal advisor investigate the possibility of renewing U-2 flights under the auspices of the Organization of American States (OAS) as a "way of legitimizing them and reducing the political consequences if a U-2 should be brought down."[51] Using the regional OAS treaty as a legal basis, U-2 flights over Cuba were soon resumed.

Argument 2: Installing the ESG is Lawful

With respect to the facts, any argument in support of the lawfulness of installing an ESG in the scenario above would focus on the 'fact' that U.S. was in the midst of a 'crisis' situation where the very survival of its overseas forces is threatened. Given this critical 'fact,' the installation of an ESG would constitute a necessary and proportional measure taken in self-defense to obtain more concrete information with regards to the capabilities and intentions of Country *X*. The ultimate goal of installing the ESG would be to prevent an armed attack against U.S. forces and the spread of conflict and instability in the region.

Based on the 'facts' of the scenario the U.S. might also argue that Country *X* had already threatened to use force as defined in Article 2(4) of the U.N. Charter. Having laid the foundation that Country *X* had threatened to use force the U.S. could then justify the installation of an ESG as an action taken in 'anticipatory self-defense' pursuant to its "inherent right of self defense" based on Article 51 of the U.N. Charter and customary international law. Indeed,

> "the collection of intelligence is a customary practice of nations, and is regarded as a vital necessity in the national security process. Intelligence collection is accomplished pursuant to the inherent right of self-defense, as codified in Article 51 of the United Nations and similar provisions in regional organization treaties. Nations collect intelligence to deter or minimize the likelihood of surprise attack; to facilitate diplomatic, economic, and military action in defense of a nation in the event of hostilities; and, in times of 'neither war nor peace,' to deter or defend against actions by individuals, groups, or a nation that would constitute a threat to international peace and security..."[52]

In addition to the foregoing, the U.S. could point out that its actions were in accord with the *purposes* of the U.N. as set forth in Article 1, namely,

> "to maintain international peace and security and to that end...take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about, by peaceful means, in conformity with the principles of justice and international law, ...settlement of...situations which might lead to a breach of the peace."[53]

Of note, some critics would argue that recourse to self-defense under Article 51 "is not vindicated by any violation of international law short of an armed attack."[54] Moreover, others point out that neither 'mere' mobilization by a potential adversary nor 'bellicose utterances' can justify self-defense within the framework of Article 51.[55] However, "there is a strong school of thought maintaining that Article 51 only highlights one form of self-defense (viz. a response to an armed attack), and that it does not negate other patterns of legitimate action in self-defense vouchsafed by customary international law."[56]

Remedies available to Country X: Anticipating that Country *X* would argue that the installation of the ESG amounted to a "threat or use of force," the U.S. would counter that the installation of an ESG does not, of itself, amount to a "threat or use of force" as the ESG is comprised of sensors only and no weapons platforms. Indeed, after the Soviet Union shot down a U.S. U-2 over it territory during peacetime in 1960, the U.N. Security Council held that the U-2 flight was a violation of Soviet airspace but not "an illegal use of force contrary to Article 2(4)" of the U.N. Charter.[57] As such, the U.S. would argue that if Country *X* detected the ESG, its response would have to be necessary and proportional. Country *X* could not *legally* use the installation of an ESG inside its territory as a legal pretext for an armed attack against U.S. forces or the territory of a U.S. ally. Rather, Country *X* would be limited to less aggressive means of response such as requesting the removal of the ESG combined with an apology and some form of compensation or, at most, the physical destruction of the ESG *only*.[58]

Other Legal Challenges Posed by NCW

This paper has only focused on only one, albeit critical, legal issue posed by NCW. In its entirety, NCW and its underlying key components bring to the fore a myriad of unsettled legal questions due to the simple fact that the law has not yet caught up with technology. For example, one obvious issue raised by emerging Navy net-centric doctrine revolves around what justifiable courses of action would be available to the U.S. to defend an ESG installed prior to hostilities. Moreover, if the U.S. were to obtain 'unambiguous warning' that another nation was about to engage in an armed attack inimical to U.S. interests, what actions could it lawfully undertake?

Additionally, it is readily apparent that NCW is focused on leveraging both information and space technologies. While it is true that information operations, to include computer network attack and defense (CNA/CND), and space operations have recently become 'hot topics' for legal analysts both inside and outside the Department of Defense (DoD), these and related issues have yet to be fully explored in the context of NCW as envisioned by the Navy. For example, Navy net-centric doctrine calls for the use of offensive information operations to assist in gaining information superiority, to assure access to the battlespace, and as part of its effects-based operations. "To the theater campaign or operations planner who must wrestle with issues regarding the use of information warfare and protection from the enemy's potential use of it, theoretical discussions of information warfare and the law are a thin gruel when weighed against the need for firm guidelines, rules of engagement, and policy."[59]

> As such, certain fundamental questions such as: What constitutes an act of information warfare? What are 'force,' 'armed attack,' or 'armed aggression' (key words used in the U.N. Charter) in the Information Age? Does 'war' between states require physical violence, kinetic energy, and human casualties? And how will long-established legal principles, such as national sovereignty and the inviolability of national boundaries, be affected by the ability of cyberspace to transcend such concepts?[60]

Each of these questions raise pertinent legal issues that need to be further explored with respect to Navy net-centric operations.

Future net-centric operational commanders will also want to know how a potential adversary might lawfully act in response to U.S. net-centric operations. For example, a Commander in Chief (CINC) vested with the authority to order a CNA would want to know what rights inured in the nation 'attacked.' Similarly, a net-centric JTF commander might want to interfere with or destroy the space assets of a potential adversary (or a third country's 'commercial assets' which the adversary is known to rely on). If so, what legal rights would

the adversary (or the third country) have if such operations were conducted prior to an armed attack by the adversary nation?

Additionally, current Navy net-centric doctrine stresses the desirability of a forward leaning posture, a more aggressive mindset, self-synchronization, and simultaneous vice sequential engagement.[61] In such an environment the potential exists for critical decisions to be pushed down the chain of command. Moreover, given that NCW at its essence is about increasing the speed of decision-making, it seems likely that the time available to make crucial decisions such as the installation of an ESG prior to hostilities, the initiation of a CNA, or the unleashing of massive amounts of firepower directed against targets on land, water and in space will be compressed. Perhaps further complicating matters, strategic, operational, and tactical commanders may possess a "common operating picture" of the battlespace that could lead to confusion as to who has the ultimate authority to order US offensive operations across the spectrum, including space and cyber-space.[62] Given these possibilities, one might question whether or not a transition to network-centric operations entails a need to conduct a wholesale review of current U.S. ROE as well as the relatively cumbersome ROE process.

Finally, what of our potential coalition partners in the brave new world of NCW? Given the fact that many of our allies already have differing viewpoints concerning the legal application of military power and ROE, doesn't it seem likely that NCW will usher in a whole new range of legal issues that could contribute to potential dissention?

The foregoing list of legal challenges posed by NCW is nowhere near exhaustive. That fact alone supports the notion that any process of evolution toward Navy NCW must involve

the systematic legal analysis of its underlying concepts to ensure the most efficient evolution of NCW technology and operational doctrine.

Recommendations

Since 1997, the CNO, the President of the Naval War College, as well as other military and civilian authors have combined to publish numerous books and articles concerning the positive and negative potential of NCW as a whole and in relation to the various warfare communities. In stark contrast, there has been little public discourse concerning either the legal challenges posed by NCW or the *process* by which the Navy will attain a NCW capability, which some believe is as critical as focusing on the potential of NCW.[63] The concepts underpinning the Navy's current vision of net-centric operations raise numerous legal issues. As such, similar to one recent commentator who argued that NCW must incorporate "human factors" into the NCW design process from the outset, this article suggests that 'legal factors' must be taken into consideration at the outset of NCW design process.[64]

NCW proponents should have no trouble with this simple proposition. In describing the transformation process toward NCW, VADM Arthur K. Cebrowski and John Garska observed that technology insertion is often "ahead of and disconnected from joint and service doctrine and organizational development."[65] Because this "problem is cultural and systemic," a "process for the co-evolution of technology, organization and doctrine is required."[66]

If this sentiment is correct then it is incumbent upon Navy leadership to request that its legal community gain a better appreciation and understanding of the types of operational legal challenges that the Navy is likely to face in the future. The responsibility would then

lie with the Navy Judge Advocate General to develop an appropriate training pipeline that would ensure that lawyers with the requisite technical and legal expertise were positioned to offer the best counsel possible to assist the Navy in its transition to NCW.[67]

Unquestionably Fleet, Battlegroup, and other service judge advocates (JAGs) must continue to participate in FBE's and wargames, not only to work ROE issues, but to critically analyze the underpinning concepts and doctrines involved in the exercises. Such 'after action' legal critiques, which would include legal concerns raised by operational participants, should then be compiled and consistently reviewed by a more permanent body of legal experts which should be established solely to assist with the development of Navy NCW doctrine. This permanent panel of experts would also ensure that the legal resources earmarked for NCW assessment and development was effectively applied and would coordinate with other services and agencies involved in analyzing legal issues surrounding future warfare concepts to ensure a synergy amongst the various sources articulating legal positions.

Additionally, within the Navy, the other services, DoD, the State Department, private 'think-tanks,' intelligence agencies, and law schools there resides a formidable reservoir of legal talent that could be tapped to help address NCW legal issues. These resources, in addition to others, such as retired JAGs specializing in operational law, are all potential players that could factor into the systematic legal review of Navy net-centric concepts.

As the Navy continues to train major staffs in the art and science of JTF command, it ought to consider incorporating some training on the legal issues a net-centric JTF commander might expect to have to deal with in the future. As more senior level operators and staff judge advocates (SJA's) become attuned to the operational and legal challenges

posed by NCW, the pool of officers available to address the legal challenges posed by NCW will only increase.

Lastly, the Navy must ensure that operators and legal experts from our major allies are integrated in some manner into the NCW design process.

Conclusion

Today it seems to be widely accepted that, when planning a JTF operation, the better practice is to ensure that the SJA works from the outset with other members of the joint staff to develop mission ROE. Why is this so? The answer is simple. Because so many potential aspects of a mission plan could be impacted by domestic and international law, it only makes sense to ensure that legal issues are raised and analyzed, not in a vacuum or after the plan is devised, but rather concurrently with the actual planning. Not only is this the most effective and efficient practice but, if ROE are prepared in isolation from actual planning, the dichotomy could have disastrous consequences.[68]

Applying the 'lesson learned' concerning the efficient development of ROE, this article stands for the simple proposition that, in order to ensure the most effective and efficient development of Navy net-centric technology and doctrine, legal experts must work concurrently with others from the outset.

Future net-centric JTF commanders have a vested interest in ensuring that the legal implications of NCW on factor space, time, and forces have been thoroughly considered. Current and future international and domestic law might limit the ability of net-centric commanders to optimize the "Capstone Concepts" of NCW. If the technological and doctrinal aspects of NCW continue to rapidly evolve without regard for the legal challenges, the Navy might find itself in a position where it has invested a tremendous amount of time

and money developing a system of sensors and platforms that cannot be employed as envisioned due to legal constraints.

If nothing else, it should now be evident that NCW encompasses a wide variety of complex legal issues that must be addressed prior to the actual employment of NCW concepts. This paper focused on only one legal challenge, the installation of an ESG prior to hostilities, in an effort to highlight the impact that international and domestic law could have on the development of future technology and operational doctrine.

If ADM Cebrowski is correct in discerning that that NCW is "the emerging military response to the information age" whose "time is at hand," then the time is now to begin systematically considering the legal challenges posed by NCW. Lessons from the past have shown that technology, doctrine, and organization should not evolve autonomously. Rather, the more prudent course is to provide for the co-evolution of this triumvirate. Part of this co-evolution entails a rigorous legal analysis of the underlying concepts of NCW. As such, a framework to integrate this legal analysis into the on-going evolution of NCW is mandatory and the appropriate resources should be applied.

If the Navy fails to take this simple yet significant step now it risks having to re-learn old lessons of ineffectiveness and inefficiency all over again. Similar to allowing ROE to be developed in isolation from actual planning, the dichotomy of allowing NCW technology and doctrine to evolve in isolation from legal analysis could have disastrous results. Why take the risk when the alternative is simple and inexpensive?

NOTES

[1] ADM Jay L. Johnson, Chief of Naval Operations (CNO), USN, Address, U.S. Naval Institute Annapolis Seminar and 123rd Annual Meeting, Annapolis, MD: 23 April 1997. *See also* VADM Arthur K. Cebrowski and John Garstka, "Network Centric Warfare: It's Origin and Future," U.S. Naval Institute Proceedings (January 1998): 29.

[2] VADM Arthur K. Cebrowski, USN, "Network-centric Warfare: An Emerging Military Response to the Information Age." Address, 1999 Command and Control Research and Technology Symposium: 29 June 1999.

[3] Cebrowski and Garstka, 34.

[4] Naval War College Faculty, "Network Centric Operations: A Capstone Concept for Naval Operations in the Information Age," (September 2000). Prepared as a "Smooth Draft" for presentation to students at the Naval War College. For the purposes of this article the author refers to this "Smooth Draft" as encapsulating the Navy's current "vision" of network-centric operations.

[5] CDR William K. Lescher, USN, "Network-Centric: Is It Worth the Risk?" U.S. Naval Institute Proceedings (July 1999): 62.

[6] "First, as a matter of domestic politics, the U.S. has a largely legal culture. The U.S. Government is described as one of laws; in public political rhetoric acts are routinely described and discussed in legal terms, and characterizing an act as illegal can be a harsh and potentially damaging criticism. Second, as a matter of domestic law, international law is as much a part of the law of the land as are the statutes that Congress enacts. Third, given the U.S. Government's apparent preference in the post-Cold War era (and even before) for acting militarily under the auspices of international coalitions or the United Nations, its prospects for obtaining such auspices are greater when it can persuade other nations that its actions are legal and those of its foes are not. Finally, as the preeminent world power, and one particularly dependent upon information systems, the U.S. has a stake in the international status quo. To the extent international law helps to provide stability and protect critical information systems, it may benefit U.S. interests." Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, Information Warfare and International Law (Washington, DC: National Defense University Institute for Strategic Studies, Command and Control Research Program, 1998), 15.

[7] Naval War College Faculty, 1. "Information superiority" is defined as that degree of dominance in the information domain that permits the U.S. to conduct operations without effective opposition.

[8] Ibid., 8. *See also* Cebrowski and Garstka, 32-33.

[9] Ibid., 1-7. Network Centric Operations "can be broadly described as deriving power from the rapid and robust networking of well-informed, geographically dispersed warfighters. They create overpowering tempo and precise, agile style of maneuver warfare. Using effect-based operations, the aim is to sustain access and to decisively impact events ashore."

[10] Ibid., 7.

[11] Ibid., 8.

[12] Ibid., 10. *See also* Cebrowski and Gartska, 33.

[13] Ibid.

[14] Ibid.

[15] Ibid., *See also* 18.

[16] Ibid., 8.

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] Cebrowski and Gartska, 40.

[21] Dr. Alberto R. Coll, Naval War College, Memorandum for Global 2000 NCA Participants, 12 July 2000.

[22] *See* Abram Chayes, The Cuban Missile Crisis, International Crisis and the Role of Law, (Lanham, MD: The American Society of International Law University Press of America 1987).

[23] Ibid., 27.

[24] Customary law is that body of rules nations consider binding on each other given the past practice of nations in the international arena.

[25] Chayes, 22.

[26] Ibid.

[27] Robert F. Kennedy, Thirteen Days, A Memoir of the Cuban Missile Crisis, (New York: W.W. Norton and Co., 1971). For example, according to the author, with respect to U.S. actions during the Cuban Missile Crisis, it "was the vote of the Organization of American States that gave a legal basis for the quarantine. Their willingness to follow the leadership of the United States was a heavy and unexpected blow to Krushchev. It had a major psychological and practical effect on the Russians and changed our position from that of an outlaw acting in violation of international law into a country acting in accordance with twenty allies legally protecting their position."

It is often argued that, during the Cold War, U.S. lawyers crafted "disingenuous" legal briefs in an effort to at least provide a pretense of legality for U.S. covert actions. *See* Sherry Sontag, Christopher Drew, Annette L. Drew, Blind Man's Bluff, The Untold Story of American Submarine Espionage, (New York: Harper Paperbacks 1998), 245, 264.

[28] John N. Moore, Fredrick S. Tipson, and Robert F. Turner, National Security Law, (Durham, NC: Carolina Academic Press 1990), 433.

[29] Ibid., 434.

[30] Ibid.

[31] Ibid., 433-434.

[32] Ibid., 433.

[33] Ibid.

[34] Statement by the President, 10 March 1983 as recorded in Annotated Supplement to the Commander's Handbook on the Law of Naval Operations, Newport, RI: Naval War College Ocean's Law and Policy Department, (November 1997): Annex A1-3, p. 1-18.

[35] United Nations Conference on the Law of the Sea, 3d, United Nations Convention on the Law of the Sea, A/CONF. 62/122 (n.p.: 1982), Article 3.

[36] Ibid. Articles 17-25.

[37] Ibid., Article 19.

[38] Ibid., Article 20.

[39] Ibid., Article 112.

[40] Ibid., Preamble.

[41] Ibid., Article 2. *See also*, Department of the Navy, Office of the Chief of Naval Operations and Headquarters, U.S. Marine Corps, and Department of Transportation, U.S. Coast Guard, The Commander's Handbook on the Law of Naval Operations, Naval Warfare Pub. 1-14 M: (October 1995), 1-8, and Moore, Tipson, Turner, 439.

[42] Moore, Tipson, Turner, 439.

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] The Charter of the United Nations, Article 2(4).

[47] The Charter of the United Nations, Article 51 states "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

[48] *See* Michael R. Beschloss, Mayday The U-2 Affair, The Untold Story of the Greatest US-USSR Spy Scandal, (New York: Harper and Row 1986); Sontag, Drew and Drew; and The Columbus Dispatch, 25 September 1992, sec. A, p. 10, The Washington Post, 29 October 1981, sec. A, p. 23, The New York Times, 1 November 1981, sec. 1, p. 13, The New York Times, 3 November 1981, sec. A, p. 1, The New York Times, 7 November 1981, sec. 1, p. 3, The New York Times, 11 November 1981, sec. A, p. 3, The New York Times, 12 November 1981, sec. A, p. 12, The New York Times, 6 May 1982, sec. A, p. 2, The Financial Times (London), 6 October 1982, sec. 1, p. 3, and The New York Times, 18 October 1982, sec. A, p. 3.

Moreover, the fact that, for example, the Soviets apologized and paid compensation when one of its submarines was found stranded in Swedish territorial waters provides some evidence that nations recognize that violating another nation's sovereignty is not lawful. *See* The New York Times, 6 May 1982, sec. A, p. 2 and The Christian Science Monitor, 3 October 1981, p.1.

[49] Sontag, Drew, and Drew, 233,248. *See also* Chayes, 19.

[50] *See* Chayes.

[51] Ibid. 19.

[52] Moore, Tipson, Turner, 433.

[53] The Charter of the United Nations, Article 1.

[54] Yoram Dinstein, War, Aggression and Self Defense, 2nd ed. (Cambridge, UK: 1994), 184.

[55] Ibid.

[56] Ibid., However, the author argues that the leading opinion among scholars is that the right of self-defense is circumscribed to counter-force stimulated only by an armed attack.

[57] Moore, Tipson, Turner, 439.

[58] The Ney York Times, 6 May 1982, sec. A, p. 2, The Christian Science Monitor, 3 October 1981, p. 1.

[59] Greenberg, Goodman, Soo Hoo, xii-xiv.

[60] Ibid.

[61] *See* Cebrowski and Gartska and Naval War College Faculty.

[62] Ibid.

[63] Lescher, 59. The author argues that "(e)xplicit consideration of the process by which we will attain an NCW capability is as crucial as focusing on the outcomes we hope to achieve." Admittedly, public discourse may be limited by the classified nature of certain aspects of NCW. However, arguably the bulk of NCW legal challenges can be addressed in unclassified forums.

[64] Commander Alan D. Zimm, USN (Ret.), "Human-Centric Warfare," U.S. Naval Institute Proceedings (May 1999): 31.

[65] Cebrowski and Gartska, 35.

[66] Ibid., 35.

[67] It should not be overlooked that, to some degree, the Navy already has begun to integrate legal analysis with NCW development. Battlegroup and other service JAG's have participated in some fleet battle experiments (FBE's) and war-games, particularly with respect to ROE development. Additionally, a Navy JAG has been assigned to the Navy Warfare Development Command (NWDC) which has been tasked to lead the Navy's development of new, operational doctrine for the transition to Network Centric Operations. However, in order to ensure the most efficient and effective development of NCW doctrine, a more expansive, coordinated, and focused effort is needed.

[68] LTCOL James C. Duncan, USMC, "The Commander's Role in Developing Rules of Engagement," Naval War College Review (Summer 1999): 77.

BIBLIOGRAPHY

Alberts, David S., John J. Gartska, and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd ed. Rev., Vienna, VA: DoD C4ISR Cooperative Research Program, 1999.

Annotated Supplement to the Commanders Handbook on the Law on the Law of Naval Operations, Newport, RI: Naval War College, Ocean's Law and Policy Department, 1997.

Beschloss, Michael R., Mayday The U-2 Affair, The Untold Story of the Greatest US-USSR Spy Scandal. New York: Harper and Row, 1986.

Cebrowski, VADM Arthur K., USN, "Network-centric Warfare: An Emerging Military Response to the Information Age." Address. 1999 Command and Control Research and Technology Symposium: 29 June 1999.

Cebrowski, VADM Arthur K., USN, Garstka, John, "Network Centric Warfare: It's Origin and Future." U.S. Naval Institute Proceedings (January 1998): 29.

The Charter of the United Nations.

Chayes, Abram, The Cuban Missile Crisis, International Crisis and the Role of Law. Lanham, MD: The American Society of International Law University Press of America, 1987.

Coll, Dr. Alberto R., Memorandum to Global 2000 NCA Participants. 12 July 2000, Naval War College, Newport, R.I.

Department of the Navy, Office of the Chief of Naval Operations and Headquarters, U.S. Marine Corps, and Department of Transportation, U.S. Coast Guard, The Commander's Handbook on the Law of Naval Operations, Naval Warfare Pub. 1-14M: (October 1995).

Dinstein, Yoram, War, Aggression, and Self-Defense, 2nd ed., Cambridge, UK: 1994.

Duncan, LTCOL James C., USMC, "The Commander's Role in Developing Rules of Engagement." Naval War College Review (Summer 1999): 77.

Greenberg, Lawrence T., Seymore E. Goodman, and Kevin J. Soo Hoo, Information Warfare and International Law. Washington, DC: National Defense University Institute for Strategic Studies, Command and Control Research Program, 1998.

Humphries, LTCOL John G. USAF, "Operational Law and the Rules of Engagement in Operations Desert Shield and Desert Storm." Airpower Journal (Fall 1992): 28.

Johnson, ADM Jay L. Chief of Naval Operations (CNO), USN. Address. U.S. Naval Institute Annapolis Seminar and 123rd Annual Meeting, Annapolis, MD: 23 April 1997.

Lescher, CDR William K. USN, "Network-Centric: Is It Worth the Risk?" U.S. Naval Institute Proceedings (July 1999): 62.

Kennedy, Robert F. Thirteen Days, A Memoir of the Cuban Missile Crisis. New York: W.W. Norton and Co., 1971.

Naval War College Faculty, "Network Centric Operations: A Capstone Concept for Naval Operations in the Information Age," (September 2000).

Moore, John N., Fredrick S. Tipson, and Robert F. Turner, National Security Law. Durham, NC: Carolina Academic Press, 1990.

United Nations Conference on the Law of the Sea, 3d, United Nations Convention on the Law of the Sea, A/CONF. 62/122. n.p.: 1982.

Sontag, Sherry, Christopher and Annette Drew, Blind Man's Bluff, The Untold Story of American Submarine Espionage. New York: Harper Paperbacks, 1998.

Zimm, CDR Alan D. USN (Ret.), "Human-Centric Warfare." U.S. Naval Institute Proceedings (May 1999): 31.